FlexiWi-Fi Security Manager Using Freescale embedded System

Mustafa Kamoona and Mohamed El-Sharkawy

Electrical and Computer Engineering
Purdue School of Engineering and Technology
Indianapolis, IN 46202

Abstract— **Among the current Wi-Fi two security models (Enterprise and Personal), while the Enterprise model (802.1X) offers an effective framework for authenticating and controlling the user traffic to a protected network, the Personal model (802.11) offers the cheapest and the easiest to setup solution. However, the drawback of the personal model implementation is that all access points and client radio NIC on the wireless LAN should use the same encryption key. A major underlying problem of the 802.11 standard is that the pre-shared keys are cumbersome to change. So if those keys are not updated frequently, unauthorized users with some resources and within a short timeframe can crack the key and breach the network security. The purpose of this paper is to propose and implement an effective method for the system administrator to manage the users connected to a router, update the keys and further distribute them for the trusted clients using the Freescale embedded system, Infrared and Bluetooth modules.**

Keywords— Wi-Fi; WPS; IR; BT; TLS; RADIUS; aircrack-ng

I. INTRODUCTION

Wi-Fi (or WiFi) is a local area wireless networking technology which allows computing devices to communicate. It primarily operates using the 2.4 gigahertz and 5 gigahertz frequency bands. The Wi-Fi is defined as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) standards' [1]. However, in the networking world, any WLAN or Wireless Area Network is known as Wi-Fi even if it does not follow the IEEE standards since most of the latest WLANs are IEEE based. Many devices can use Wi-Fi, e.g. Personal Computers, video-game console, tablets, and smartphones. These can connect to a network resources such as the Internet via a wireless access point. Such an access point has a range of about twenty meters indoors to a much wider range outdoors. The indoor access point coverage can be limited to a single room if the walls block the radio signals, whereas multiple miles of range can be obtained if overlapping access points are used. Usually Wi-Fi networks are less secure than Ethernet or any other wired connections since the adversary does not need a physical connection to access the network. The network traffic that uses the transport layer security is somehow secure, however, if no security encryption is used then the internet traffic can easily be detected by adversarial intruders. Because of that, Wi-Fi has started using various encryption mythologies. Ranging from the early Wired Equivalent Encryption (WEP) which proved easy to break. Then later, higher quality protocols like (WPA, WPA2) were added.

WPA Enterprise model requires RADIUS (an authentication server) based authentication 802.1x and a Database which is a rather complicated setup and it can be burdensome to maintain. WPA Personal uses a Pre-Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. Using offline dictionary attacks, weak PSK passwords can be broken by capturing the four-way exchange messages that occur when the client reconnects after being disconnected (deauthenticated). Wireless suites such as aircrack-ng can crack a weak passphrase in a matter of hours. Other WEP/WPA crackers are Auditor Security Collection and AirSnort and. Still, if strong passphrases are used then WPA Personal takes more time to hack. The problem with Personal model is that the key administration and distribution is not easy to manage and a new enhancement should be implemented to facilitate this process.

This paper proposes and implements a way of achieving a user friendly way for the WLAN system administrator to manage the connected users and change the password easily and then enables the trusted clients to retrieve the new password on their device screen easily and securely using only the Infrared transmitter and the Bluetooth module on their device without the need to be connected to the Wi-Fi network.

This paper proceeds as follows: Section II illustrates the weak key change and distribution in the personal model. Section III reviews some related project work. Section IV introduces the proposed enhancement intended to solve this problem in the Wi-Fi networks. Section V Explains the detailed design while section VI evaluates the scheme security by analyzing the scheme's security measures, and Section VII concludes the paper.

II. THE KEY MANAGMENT AND DISTRIBUTION PROBLEM

Since the Wi-Fi personal security model can be breached with moderate resources, the admin should change the key on regular basis or as required with a new key that is not simple and easy to hack. The current implementation of this model gives the system admin very limited flexibility to manage the current password, and then distribute the new one to the trusted users that should be able to connect to the network. In the current scenario, to change the password, the admin should log in to the router through a web page and check for the currently connected

This is the author's manuscript of the article published in final edited form as:
Kamoona, M., & El-Sharkawy, M. (2015). FlexiWi-Fi Security Manager Using Freescale Embedded System. In 2015 2nd International Conference on Information Science and Security (ICISS) (pp. 1–4). https://doi.org/10.1109/ICISSEC.2015.7371003

users, if any suspicious activity is found then he should change the key a new hard-to-guess one. And here the problem of distributing this new key to all the users that are supposed to be able to connect to the network arises. The current solutions for distributing the keys including the word of mouth, printed credentials, even QR codes are easy to get to the wrong hands and might defy the whole point of changing the password as the admin will have to redo the whole operation and that can be infuriating and time consuming.

III. Related Project Work

There are many implementations that try to facilitate the security management of the Wi-Fi network, nevertheless, none of them actually solves it. One of the best current work is the Wi-Fi Protected Access or the WPS. It was meant for the users who know little of the wireless security to get connected to the network without having to enter long passwords. A major security flaw in the routers with this feature was revealed in 2011 which proved that the adversary can use a brute force attack to get the pin and hence hack the network [3]. The WPS also supports USB, NFC or push button ways of communicating the keys to the clients, but all of those methods are ways to share the keys with the users and do not target the administrator's way of managing those keys. Another recent work is the KeeWifi project, it proposes a mechanism that manages the users' connectivity to the system's router by using the NFC tag to keep a whitelist of the trusted users MAC addresses with the first one in the list being the administrator. This could be a way to facilitate the connected users management but also might lead to further security holes if the adversary has some knowledge about networking security as they can easily dump the raw wireless traffic to see the currently associated MAC addresses using simple hacking applications like aircrack-ng and then spoof the MAC address and furthermore if the administrator MAC address is the one that was spoofed, the unauthorized user can kick the original admin out and take over the whole system control.

IV. Proposed Scheme

The proposed solution is to use an embedded system which can be accessed remotely by the authorized users to completely manage the router. Using the IR module on the wireless device, the admin can send commands to the embedded system to get a list of the connected users, get the current password and even change the password to a predefined length randomly generated password. The output of the commands will be sent back via Bluetooth to the admin screen. The clients on the other hand, can send only one IR command to get the current Wi-Fi password and display it on their screen using the Bluetooth. The admin and users will have to have a line of sight visibility with the embedded system which in turn will be connected via Ethernet to the router. Below is the flow chart of the admin's and client's sequence of operation.

V. Detailed Design

The full system design and connectivity is shown below. The router is dd-wrt UNIX based router and is capable of using the telnet protocol and running shell scripts. The embedded system used is the Freescale freedom k64f that has an ARM processor and multiple code libraries are already available online for its C/C++ code. The IR receiver is a simple photo resistor followed by a low pass filter stage to demodulate the IR signals sent from the admin's or client's Android device. The IR signal is a Pulse Width Modulated (PWM) square wave with only two patterns to represent the digital levels 0 and 1. The Bluetooth master module is a serial to Bluetooth module HC-05 that is used to switch the serial output to BT packets via the built in Bluetooth stack, it is configured to be paired only with one device at a time to prevent data sniffing. It is also set to send data from only one direction that is from the embedded system to the device that sends the IR code to block any try to hack the system through the Bluetooth port. A Telnet client is installed in the embedded system and is trained to negotiate then log in to the Telnet server in the router whenever a legitimate IR command is received, upon completion of the action, the Telnet session will be terminated to hinder any router misconfiguration.

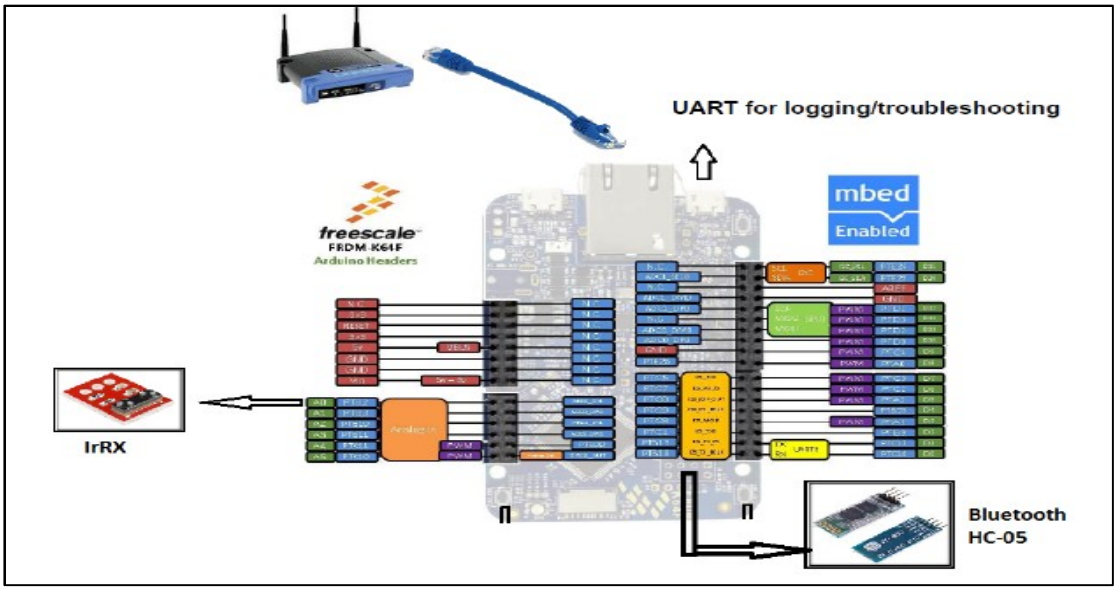

Fig. 1 FlexiWiFi System Design and Connectivity

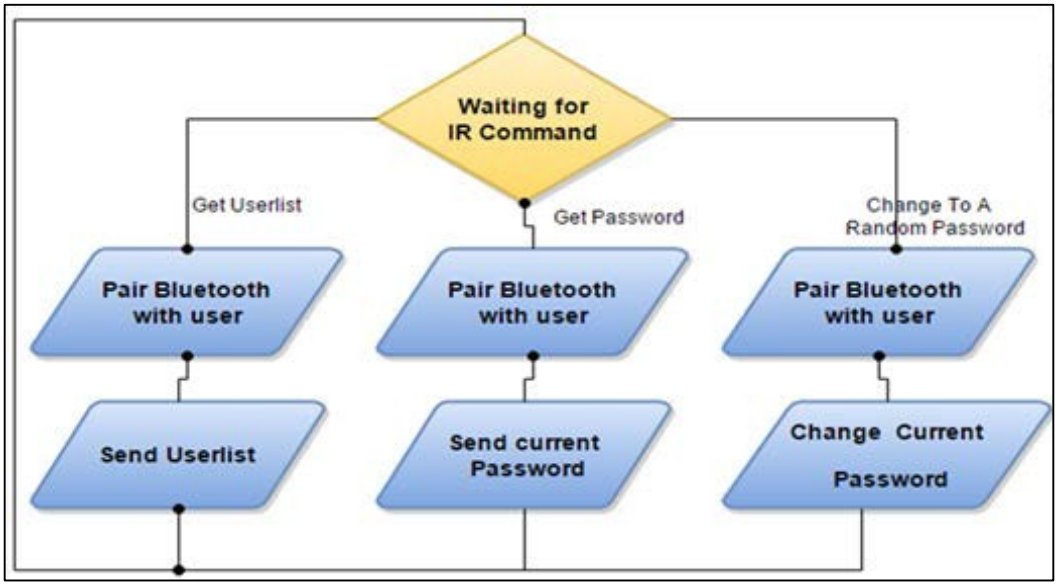

Fig. 2 Administrator's simplified Flow chart

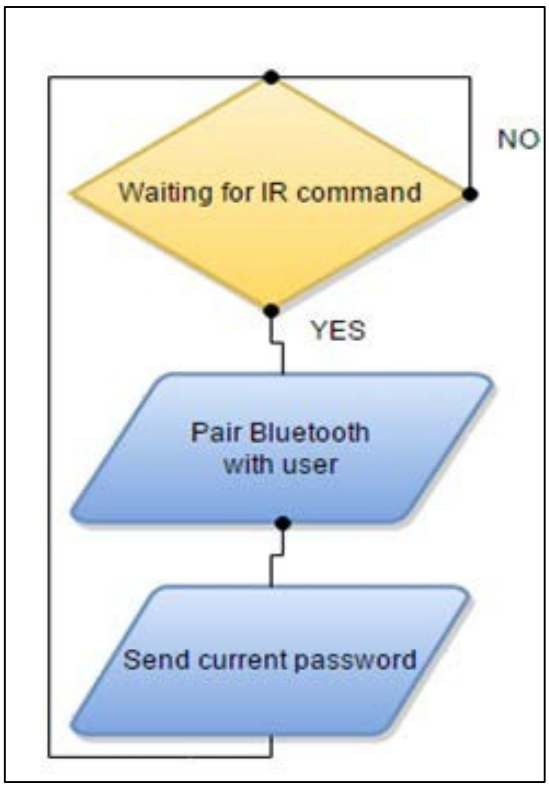

Fig. 3 Client's simplified Flow chart

VI. Security Analysis

The proposed scheme FlexiWiFi manager proves being secure as it does not modify the current WPA/WPA2 implementation, it only adds extra features that enhance the manageability of the system to make it more secure and easy to perform damage-control and recovery from a network breach. That means all current WPA/WPA2 security features will still apply plus a new security features added by the new scheme. Compared to the related projects work, multiple enhancements were performed to add a layer of extra security. Firstly the Ethernet connection between the embedded system and the router makes this connection difficult to be sniffed assuming no physical access can easily be achieved which is usually the case for personal Wi-Fi networks, this will allow an easier communication between the embedded system and the router, as simple Telnet protocol can be used.

Secondly, the IR codes used are genuine and unique to the proposed scheme as they are not used in any other IR applications. The embedded system is trained to decode the specific codes and accordingly perform the required action. Although that adds some sort of security by obscurity, but indeed it makes it difficult for the attacker to have his hands on the IR codes.

Moreover, the line of sight requirement for admin and client IR control makes it difficult for adversaries even if they have the right IR codes to send them to the embedded system. This makes the project useful in buildings with many offices but not in the same floor or where a line of sight for unauthorized users cannot be achieved with the embedded system.

Additionally, the Bluetooth module used is a master module, meaning it can be set to be paired to one and only one device at a current time. Using this approach, even though Bluetooth connections are difficult to be sniffed, it can be guaranteed that only the user who is sending the IR commands will get the desired output on their screen and no other

unauthorized users can sniff the output at the time the IR command is sent.

Furthermore, the selection of the random passwords with a predefined character set and length adds in more security. The adversary has to invest more time and resources if the WPA/WPA2 passphrase is not a simple one. The proposed scheme uses this quality by enabling the admin to increase the length of the passphrase and even include more special characters to make it even more difficult for the dictionary attacks to find the current password. An extra feature for changing the password every preset time interval like a day or a week can be implemented on demand. Which makes it a good combination if done with an adequately long strong random password.

VII. Conclusion

In order to improve the Wi-Fi personal model security and facilitates its administration, this paper proposed a scheme that helps the system admin to display the users connected to the router on his device screen and change the password to a random one to keep the system secure, the clients can get the new password to their screen as well. All that is simply done with a button press within an app which takes a couple of seconds to be performed. The system requires no change to the current implementation except adding the embedded system which in the future can be integrated to the router. This scheme proves secure and user friendly to use. Ongoing work seeks to build the app for iPhone users as the app only supports Android devices only.

References

[1] Vangie Beal, “Wi-Fi” http://www.webopedia.com/TERM/W/Wi_Fi.html April, 2008.

[2] Wi-Fi Alliance, "Securing Wi-Fi Wireless Networks with Today’s Technologies”, February, 2003.

[3] Stefan Viehböck,“Brute forcing Wi-Fi Protected Setup when poor design meets poor implementation”, December, 2011.

[4] Andrew Zafft et al., “Malicious WiFi Networks: A First Look”, Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference [1038 - 1043], October, 2012.

[5] B. Potter, “Wireless Security Future,” IEEE Security & Privacy, vol. 1, no. 4, 2003, pp. 68–72.